Fraud Awareness Alert

SunTrust

Wire Fraud Alert - Business Email Compromise

The financial services industry has recently seen a significant increase in clients falling victim to the efforts of fraudsters through a scam known as Business Email Compromise (BEC). The Internet Crime Complaint Center (IC3), a task force comprised of the FBI and other agencies, recently stated that fraudsters stole more than $200 million from businesses between October 2013 and December 2014.

What is it?

BEC is a combination of methods used by fraudsters to trick victims into moving money by disguising their efforts as legitimate. The BEC scam targets companies that regularly make wire transfer payments to foreign suppliers and businesses. Fraudsters monitor and study their selected victims prior to initiating a BEC scam, accurately identifying the individuals and protocols necessary to perform wire transfers within a specific business environment.

There are three basic tactics:

- **Email compromise** – a known email account is hacked and used to send fraudulent requests that appear to be genuine
- **Email spoofing** – emails are sent from fake, but realistic-looking, email accounts with similar-looking characters to make them harder to spot – for example: "0" (zero) for the letter "O," and capital "I" for a lower case "l."
- **Phone/mail spoofing** – a request by phone or mail is sent by fraudsters, instructing a company to send their payments on invoices to a fraudulent account.

Your business controls are your best protection against loss.

The primary variations of these tactics, each intended either to divert existing transactions or to generate new transactions to a fraudulent account, are:

- A supplier's payment information is changed to a fraudulent account, causing future invoice payments to be sent to the fraudulent account.
- Emails appearing to originate from high-level executives (e.g., CEO, CFO) are sent to staff responsible for payments requesting an urgent wire transfer to be sent to a fraudulent account.
- Emails appearing to originate from an employee's personal or business email are sent to customers requesting invoice payments to a fraudster-controlled bank account(s). Emails are usually sent to many different customers found in the employee's contact list.

Common characteristics of email compromise events:

- Businesses and their personnel who use open-source email are the most targeted.
- Hacked emails are often associated with personal, web-based email accounts.
- Hacked IP addresses are frequently traced back to free domain registrars, according to victims' reports.
- Scams are highly tailored to the target:
  - Individuals responsible for handling wire transfers in a specific business are targeted.
  - Spoofed emails very closely mimic a legitimate email request.
  - Fraudulent email requests for a wire transfer are well-worded, specific to the business being victimized, and do not raise suspicions to the legitimacy of the request.
  - Fraudulent wire transfer amounts requested are business-specific, with dollar amounts requested resembling normal business transactions to avoid raising doubt.
  - Fraudsters are aware of executives' travel schedules. Some fraudulent email requests coincided with business travel dates for executives whose emails were spoofed.

What can happen?

Simply put, **you can be tricked into sending your money to a fraudster overseas**, in a way that makes the funds virtually unrecoverable.

What can I do to prevent it?

Your business controls are your best protection against loss from business email compromise. By establishing strong controls and practicing vigilance, you have the ability to prevent your money from being taken by fraudsters.

Business Process Controls:

- Require two people to approve the movement of large sums or make changes to information that impacts the movement of funds, such as recipient information.
- Verify any requests to change recipient information with the appropriate contact prior to making the change.
- Verify important or large transactions through another method, such as a telephone call or face-to-face discussion.
- Do not reply directly to emails requesting movement of money. Instead, use the "forward" option and either type in the correct email address, or select it from your email address book to ensure the intended recipient's correct email address is used.
- Work with your financial institution(s) to implement additional security controls, such as phone verification. Phone verification will not stop a transaction you believe to be genuine, but the extra check may cause you to notice something is wrong.

Awareness:

- Cultivate an environment that empowers employees to question abnormal requests.
- Carefully review the email address of the sender of any requests to move money.
- Train your processing staff to question any requests for secrecy, bypass of normal procedures, or pressure to take action quickly.
- Be aware of sudden changes in business practices. If you are suddenly asked to contact someone through their personal email address, the request could be fraudulent. Always verify through channels other than email that you are still communicating with your legitimate business partner.

Information Security:

- Never use free, web-based email accounts for business purposes. Establish a company website domain and use it to create company email accounts. If a free, web-based email must be used, select a provider who offers multi-factor authentication.
- Limit the amount of information available to the general public about job duties and descriptions, company hierarchy, and travel details. Any discoverable information can be used to help a fraudster determine where you are most likely to be vulnerable.
- Employ good network hygiene practices, including, but not limited to, keeping your software patches up to date, using anti-virus software, and restricting entry points into your network.
- If possible, conduct all banking on a dedicated machine used for no other task. Create a dedicated virtual operating system (OS) for the sole purpose of providing a secure environment.

If it happens, what should I do?

1) **Call your financial institution**. The only chance of recovering your funds is an immediate recall by your bank. The policies of foreign financial institutions vary. Not all recalls are successful. Money is usually moved out of the destination account within minutes of arrival. Once the money has been moved, there's nothing left to be recovered.
2) **File a complaint with the Internet Crime Complaint Center** (IC3) at www.ic3.gov. The IC3 will route your case to the appropriate local law enforcement bureau. It is at the discretion of that bureau as to whether to move forward on your case.
3) **Review your business processes** to identify the gap that allowed the transaction to be submitted. Once you find the gap, close it and provide training to your staff.

As financial institutions continue to enhance their controls, fraudsters are shifting their focus to target end users more than ever. You are in the best position to protect your money against their efforts through awareness and business controls.

Remember: Once a fraudulent international wire transfer has been completed, recovery of funds is extremely unlikely.

SunTrust